ANALISA PRINSIP KERJA *MALWARE*, DETEKSI DAN PENANGANAN SERTA PERKEMBANGAN *MALWARE* UNTUK PENINGKATAN KEAMANAN KOMPUTER

SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Program Studi
Strata I pada Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh:

Heri Muslihan
NIM : L200070093

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2012

HALAMAN PERSETUJUAN

Skripsi dengan judul

ANALISA PRINSIP KERJA BEBERAPA MALWARE, DETEKSI DAN PENANGANAN SERTA PERKEMBANGAN MALWARE UNTUK PENINGKATAN KEAMANAN KOMPUTER

ini telah diperiksa, disetujui dan disahkan pada :

Hari : …….

Tanggal : ……..

Pembimbing I	Pembimbing II
Fatah Yasin,S.T., M.T.	Abdul Basith, S.T., M.T
NIP/NIK:……..	NIP/NIK:……..

HALAMAN PENGESAHAN

Analisa Prinsip Kerja Beberapa Malware, Deteksi dan Penanganan Serta Perkembangan Malware Untuk Peningkatan Keamanan Komputer

dipersiapkan dan disusun oleh

Heri Muslihan

NIM : L200070093

telah dipertahankan di depan Dewan Penguji

pada tanggal .....….

Susunan Dewan Penguji

Pembimbing I	Anggota Dewan Penguji Lain
Fatah Yasin Irsyadi, S.T.,M.T	Husni Thamrin, S.T, M.T., Ph.D
Pembimbing II	
Abdul Basith, M.T	Jan Wantoro, S.T

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal ……..

Dekan Fakultas Komunikasi dan Informatika	Ketua Program Studi Teknik Informatika
Husni Thamrin, S.T, MT., Ph.D. NIK : ….	Aris Rakhmadi, ST., M.Eng. NIK : ….

DAFTAR KONTRIBUSI

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi:

1. Dalam penulisan skripsi ini penulis akui ada peran dari teman - teman, akan tetapi peran itu hanya sebatas melengkapi yang sudah ada dan penulis kerjakan sendiri dan dikembangkan sendiri.
2. Panduan dalam pendeteksian dan penghapusan *malware* tersebut penulis dapatkan dari buku, kemudian tambahan materi dari *browsing* internet yang selanjutnya penulis kembangkan sesuai dengan kebutuhan.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggungjawab atas isi dan kebenaran daftar di atas.

Surakarta, …….

Heri Muslihan

Mengetahui:

Pembimbing I	Pembimbing II
Fatah Yasin, S.T , M.T	Abdul Basith, M.T
NIP/NIK:……..	NIP/NIK:……..

HALAMAN PERSEMBAHAN

1. *Ayah Bagiyo dan Bunda Siti Sholikah yang telah merawat, membimbing serta mendo'akan penulis dalam menjalani kehidupan ini terima kasih, dan selalu menanyakan gimana skripsinya???saat ananda pulang rumah, maafkan bila ananda belum bisa membuat bangga dan banyak melakukan kesalahan, nasehatmu akan selalu ku dengar, maafkan ananda karena ananda hanya bisa mengucapkan terimakasih banyak akan ananda ingat selalu bahwa perjalanan ananda masih panjang.*
2. *Adikku Imam Mustain yang tercinta yang selalu memberikan motivasi, semoga Allah selalu memberikan risky dan perlindungan-Nya untuk keluarga kita.*
3. *Teman-teman seperjuangan pendhoz, dadik, sukapi, bagong, adit, imunk, sopi,dll yang tidak bisa penulis sebutkan satu persatu, terima kasih atas supportnya dan bantuanya.*
4. *Teman-teman menghabiskan malam awi, bebek, kasrun kecil, kasrun gede, ucok, dll yang tidak bisa penulis sebutkan satu persatu, terima kasih atas waktunya untuk menghabiskan malam di Selero Denai.*
5. *Teman – teman satu kontrakan jarot, kutuk, pindank, mayit, yoga, terima kasih atas kebersamaannya selama hampir 5 Tahun walaupun banyak perbedaan tapi tidak membuat pecah pertemanan.*

6. Semua pihak yang telah membantu terselesaikannya skripsi ini yang tidak bisa penulis sebutkan satu persatu.

MOTTO

Hidup ini sangat singkat, lakukanlah yang terbaik jangan sia-siakan waktu dan buatlah orang disekitarkita dapat tersenyum bahagia karena hidup ini terasa sangat indah apabila

Kita dapat meringankan beban orang lain

(Penulis)

Memberilah seakan kamu berjalan di pasir tepi pantai dan menerimalah seakan kamu berpijak diatas batu yang pijakan kamu tidak akan terhapus selamanya

(Jefri Al-Buqri)

Didunia ini tidak ada yang tidak mungkin tiada kata kalah sebelum berperang, yang penting dari semua itu adalah prosesnya karena proses itulah yang akan membawa kita pada keberhasilan

(Mario Teguh)

Terkadang hidup itu sangat menyakitkan.tapi lebih menyakitkan bila kita tidak pernah berbuat apa-apa untuk kehidupan kita, jadi hargai setiap nafas yang berhembus,karna kita

tidak akan pernah tahu kapan akhir dari kehidupan ini

(Penulis)

Kita tidak bisa merubah dunia bukan berarti dunia bisa merubah kita

(Deddy Corbuzier)

Jagan kamu fikirkan apa yang akan kamu dapatkn dari orang tua kita, tetapi fikirkanlah

apa yang akan kamu berikan kepada orang tua kita

(Penulis)

KATA PENGANTAR

Dengan menggucapkan rasa syukur kepada Allah SWT. Atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini. Skripsi ini dibuat Sebagai salah satu syarat untuk memperoleh derajat Sarjana S1 Pada program studi Teknik Informatika.

Penulisan skripsi ini masih tergolong sederhana dan penulis menyadari masih banyak kesalahan didalamnya. Namun dalam pengerjaan skripsi ini penulis sudah melakukan semakasimal mungkin menurut kemampuan yang dimiliki penulis, dengan harapan dapat memberikan sumbangsih dalam dunia TI, dan semoga dapat berguna bagi secara pribadi maupun para pembaca. Penulis tidak lupa menggucapkan banyak terima kasih kepada:

1. Allah SWT. Yang selalu memberikan rahmat dan hidayah-Nya dan kesehatan yang tidak terukur.
2. Bapak Husni Tamrin, S.T.,M.T.,P.hd selaku dekan Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta.
3. Bapak Aris Rakhmadi, S.T, M.Eng selaku ketua jurusan Informatika Universitas Muhammadiyah Surakarta.
4. Fatah Yasin, S.T., M.T selaku dosen pembimbing I yang memberikan bimbingan dan pengarahan kepada penulis sehingga dapat menyelesaikan skripsi ini.

5. Abdul Basith, S.T., M.T selaku dosen pembimbing II yang memberikan bimbingan dan pengarahan kepada penulis sehingga dapat menyelesaikan skripsi ini.
6. Bapak Bagiyo, Ibu Siti Sholikah, Adik Imam Mustain yang terus memberikan do'a dan motifasinya sehingga penulis dapat menyelesaikan skripsi ini.
7. Teman-teman perjuangan pendhoz, dadik, sukapi, bagong, adit, imunk, sopi, dll yang tidak bisa penulis sebutkan satu persatu,terimakasih atas supportnya.
8. Teman-teman menghabiskan malam awi, kasrun kecil, kasrun gede, ucok, bebek, dll yang tidak bisa penulis sebutkan satu persatu, terimakasih atas waktunya dalam menghabiskan malam di Selero Denai.
9. Teman – teman satu kontrakan jarot, kutuk, pindank, mayit, yoga, terima kasih atas kebersamaannya selama hampir 5 Tahun walaupun banyak perbedaan tapi tidak membuat pecah pertemanan.
10. Semua pihak yang telah membantu terselesaikannya skripsi ini yang tidak bisa penulis sebutkan satu persatu.

Dalam penyusunan skripsi ini ada beberapa kesulitan dan hambatan, namun penulis berusaha untuk menyelesaikan skripsi ini dengan semangat penulis dan bantuan dari teman-teman semaksimal mungkin menurut penulis sehingga penulis dapat menyelesaikan skripsi ini.

Penulis menyadari skripsi ini jauh dari sempurna karena “tidak ada gading yang tak retak” banyak sekali kekurangan dan kesalahan penulisan skripsi ini, oleh karena itu penulis memohon maaf sebesar-besarnya atas kesalahan tersebut.

Terima Hasih.

Surakarta, Januari 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL i

HALAMAN PERSETUJUAN ii

HALAMAN PENGESAHAN iii

MOTTO iv

KATA PENGANTAR v

DAFTAR ISI vi

DAFTAR GAMBAR ix

DAFTAR TABEL x

ABSTRAKSI xi

BAB I PENDAHULUAN 1

A. Latar Belakang 1
B. Rumusan Masalah 4
C. Batasan Masalah 4
D. Tujuan Penelitian 4
E. Manfaat Penelitian 4
F. Sistematika Penulisan Laporan Penelitian 5

BAB II TINJAUAN PUSTAKA 7

A. Telaah Pustaka 7
B. Landasan Teori 8
    1. Virus 8
    2. Worm 12
    3. Trojan Horse 15

BAB III METODE PENELITIAN 18

A. Waktu dan Tempat penelitian 18
B. Peralatan Utama dan Pendukung 18
C. Alur Penelitian 19
1. *Virus Conficker* 21
2. *Worm Shortcut* 24
3. *Trojan (W32/Obfuscated.J)* 29

BAB IV ANALISA 32

A. Hasil Penelitian 32
1. *Virus Conficker* 32
2. *Worm Shortcut* 34
3. *Trojan (W32/Obfuscated.J)* 37
B. Pembahasan 41
1. *Virus (confiker)* 41
2. *Worm (stuxnet)* 44
3. *Trojan (W32/Obfuscated.J)* 45

C. Perkembangan *Virus*, *Worm* dan *trojan horse* 49
1. *Virus* 49
a. *Virus Melisa* 49
b. *Virus Phising* 50
2. *Worm* 52
a. *ILOVE YOU* 52
b. *Stuxnet* 53
3. *Trojan Horse* 55
a. *Back Orifice* 55
b. *Trojan Downloder* 58

BAB V KESIMPULAN DAN SARAN 60

A. Kesimpulan 60
B. Saran 61

DAFTAR PUSTAKA

DAFTAR TABEL

Table 4. 1. Perbandingan *virus*..... 51

Table 4. 2. Perbandingan *worm*..... 55

Table 4. 3. Perbandingan *Trojan Horse*..... 59

DAFTAR GAMBAR

Gambar II.1. Kronologi *worm* 14

Gambar III.1.Dagram penelitian 20

Gambar III.2. Aksi *conficker* mematikan *servise windows* 21

Gambar III.3. *Norman* mendeteksi *conficker* 22

Gambar III.4. *Script* untuk penanganan *conficker* 23

Gambar III.5. *Norman* tidak mendeteksi *conficker* 24

Gambar III.6. *Icon flasdisk* yang dirubah *shortcut* 24

Gambar III.7.*USB Flash* saat diakses keluar *"Access is denied"* 25

Gambar III.8. Pesan *error* saat akses *USB Flash* 25

Gambar III.9. *Scan* dengan *norman* 26

Gambar III.10. *Key* pada *registry* yang akan dihapus 27

Gambar III.11. Merubah *key* yang telah dirubah oleh *shortcut* 28

Gambar III.12. *Norman* tidak mendeteksi adanya *shortcut* 28

Gambar III.13. *Dr.Web.* mendeteksi varian baru dari *W32/Obfuscated* 30

Gambar III.14. *Script* yang digunakan untuk *repair W32/Obfuscated* 30

Gambar III.15. *Dr.Web.* tidak mendeteksi adanya *trojan* 31

Gambar IV.1. *Norman* mendeteksi *conficker* 32

Gambar IV.2. *Script* untuk *conficker* 33

Gambar IV. 3. *Norman* tidak mendeteksi adanya *conficker* 33

Gambar IV. 4. *Norman* mendeteksi *shortcut* 35

Gambar IV. 5. *Norman* tidak mendeteksi *shortcut* 37

Gambar IV. 6. Proses *scan* yang dilakukan *Dr.Web*..... 39

Gambar IV. 7. *Script* yang digunakan untuk me-*repeir registry* 40

Gambar IV. 8. Gambar *drive* bersih dari *trojan*..... 40

Gambar IV. 9. *Script* untuk virus *conficker* 42

Gambar IV. 10. *Script* untuk *trojan* 46

Gambar IV. 11. Gambar *virus melisa* 50

Gambar IV. 12. Gambar *virus phising* pada *facebook*..... 51

Gambar IV. 13. Gambar *worm ILOVE U* 53

Gambar IV. 14. *File wista* bertambah besar dan mengelembung..... 55

Gambar IV. 15. Tampilan *home Back Orifice* 58

Gambar IV.16. Gambar file trojan downloader 59

ABSTRAKSI

Kebanyakan dari user atau pengguna komputer hanya tahu menghapus malware semacam *virus, worm,* dan *trojan horse* menggunakan anti – *virus* yang sudah terinstal pada komputer, mereka tidak mengerti bahwa ada langkah yang belum selesai. Langkah tersebut adalah membenahi *registry* yang telah dirusak oleh *malware*, karena setiap *malware* yang menyerang sebuah komputer akan merusak *registry* untuk melindungi keberadaannya agar tidak mudah terdeteksi oleh anti - *virus*

Komponen penting yang digunakan adalah *software norman removal tool* dan *Dr.Web* yang digunakan untuk pendeteksian keberadaan *virus*, *worm,* dan *trojan horse*. Penelitian dilakukan dengan meng-*install* anti-*virus* untuk pendeteksian dan penghapusan kemudian merubah *registry* yang telah dirubah oleh *malware* tersebut. Ada beberapa *malware* yang dalam penanganannya diharuskan men-*download security patch* dari *windows* untuk menutup lubang yang digunakan *malware* sebagai celah keamanan dari *windows.*

Analisa yang dilakukan adalah pendeteksian dan penanganan terhadap *malware* yang ada pada komputer. Dari hasil penelitian penulis dapat mengetahui bahwa dalam penanganan *malware* tidak cukup menggunakan anti-*virus* karena *malware* tersebut sudah melakukan perubahan dalam *registry* jadi *user* harus merubah *registry* yang telah dirubah oleh *malware* dengan menuliskan script tertentu dan meng-*install security patch* dari *windows.*

Kata kunci : *Virus, Worm, Trojan Horse, Registry, Security Patch.*